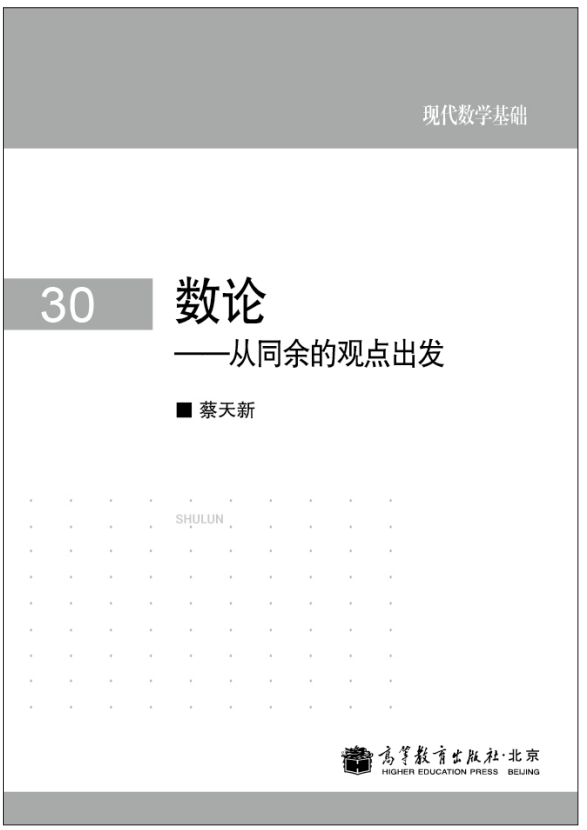
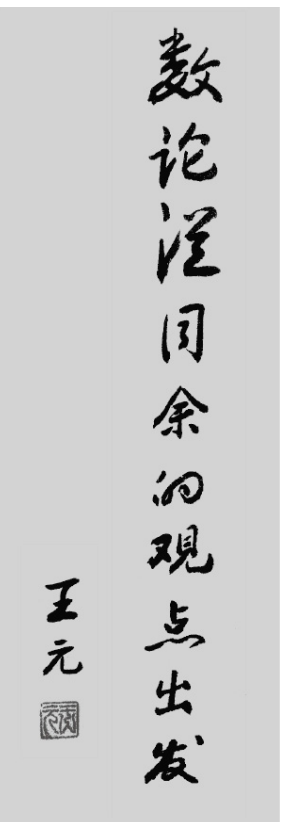
数是我们心灵的产物

蔡天新



《数论——从同余的观点出发》



王元先生扉页题词

编者按 *本文是蔡天新教授为他新近出版的著作《数论——从同余的观点出发》(高等教育出版社，2012年9月)所作的导言，在这本基础数论教程里，每小节后面都有补充读物，从中介绍了数论研究的新方法，并就若干经典数论问题提出自己大胆新颖的想法或延拓，部分结果发表后引起数论界同行的关注，包括菲尔兹奖得主阿兰·贝克在内的名家都予以褒扬。蔡天新教授认为，他之所以能在近年取得自我突破，部分原因是对数学史和数学文化进行了学习和探讨，这提升了他的想象力，促进了他的数论研究。*

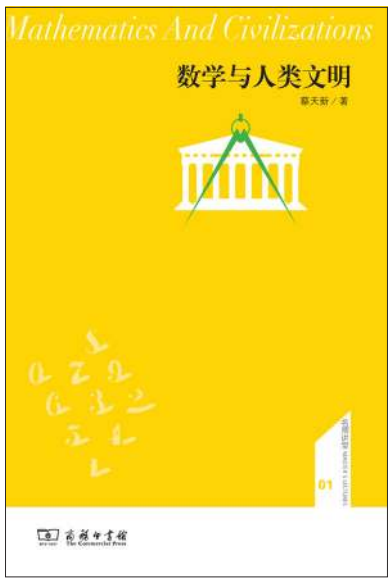
将近一个世纪以前，美国出生的英国数学家莫德尔在一篇随笔中写道："数论是无与伦比的，因为整数和各式各样的结论，因为美丽和论证的丰富性。高等算术（数论）看起来包含了数学的大部分罗曼史。如同高斯给索菲·热尔曼的信中所写的，'这类纯粹的研究只对那些有勇气探究她的人才会展现最魅人的魔力'。"或许有一天，全世界的黄金和钻石会被挖掘殆尽，可是数论，却是用之不竭的珍宝。

1801年，24岁的德国青年高斯出版了《算术研究》，从而开创了数论研究的新纪元。这部伟大的著作曾投寄到法国科学院而被忽视，但高斯在友人的资助下将它自费出版了。在那个世纪的末端，集合论的创始人康托尔这样评价："《算术研究》是数论的宪章……高斯的出版物就是法典，比人类其他法典更高明，因为无论何时何地从未发觉出其中有任何一处错误。"高斯自己则赞叹，"数学是科学的皇后，数论是数学的皇后。"

这部著作的开篇即定义了同余，任意两个整数 a 和 b 被认为是模 n 同余的，假如它们的差 $a-b$ 被 n 整除。高斯首次引进了同余记号，他用符号"≡"表示同余。于是，上述定义可表示为

$$a\equiv b(\mathrm{mod}\ n)$$

有了这个方便的同余记号以后，数论的教科书显得更加简洁美观。今天，基础数论教材的开篇大多介



左：《数学与人类文明》；右：《数字与玫瑰》修订版，两本同是 2012 年秋冬由商务印书馆出版的数学文化著作，它们与《数论》构成作者的 2012 数学三部曲

绍整除或可除性。整除与同余式也构成了本书的前两章，实际上，整除拟或带余数除法（在中国、印度和希腊等地有着各自的渊源故事和名称）

$$a\equiv bq+r,\ 0\le r<b$$

也等价于同余式 $a\equiv r(\mathrm{mod}\ b),\ 0\le r<b$。

接下来的三章，无论不定方程，还是原根和指标，均与同余有关，更不要说一次、二次和 n 次剩余了。不仅如此，初等数论中最有名的定理，除了算术基本定理以外，均与同余有关。例如，欧拉 - 费尔马定理、威尔逊 - 高斯定理、拉格朗日定理和中国剩余定理，后者的准确名字应为孙子 - 秦九韶定理，或秦九韶定理（参见第 3 章第 1 节）。

进入第 3 章以后，我们讲述了高斯最得意的、花费许多心血反复论证（共 8 次）的二次互反律，高斯称其为“算术中的宝石”。设 p 和 q 是不同的奇素数，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}$$

这里 (p/q) 为勒让德符号，当它取 1 或 -1 分别表示二次同余式 $x^2\equiv p(\mathrm{mod}\ q)$ 有解或无解。这个结果是完美无缺的，我们用几何和代数方法给出两个证明。在第 6 章我们介绍了一个新的同余式，她有着同样美丽的对称性。设 p、q 为不同的奇素数，则

$$\begin{pmatrix} pq-1 \\ (pq-1)/2 \end{pmatrix}\equiv\begin{pmatrix} p-1 \\ (p-1)/2 \end{pmatrix}\begin{pmatrix} q-1 \\ (q-1)/2 \end{pmatrix}(\mathrm{mod}\ pq)$$

此处 ( ) 为二项式系数。

除了引进同余符号，高斯还给出了正多边形作图方法和原根存在的充要条件，前者是有着两千多年历史的数学悬案，后者的理论虽较完整仍可以增补（如原根的乘积、求和同余），这些在本书的第 4 章第 5 节和第 5 章均有展示。说到原根的存在性，少不了素幂模同余式，本书的第 7 章给出了不少素幂模甚或整数幂模的崭新公式，包括拉赫曼同余式的推广，后者在怀尔斯的证明之前一直是研究费尔马大定理的主要工具。诚如加拿大和爱尔兰两位同行指出，这一推广（指从素幂模到整数幂模）是 1906 年以来的第一次。又如，设 n 是任意奇数，我们发现并证明了

$$(-1)^{\phi(n)/2}\prod_{d|n}\begin{pmatrix} d-1 \\ (d-1)/2 \end{pmatrix}^{\mu(n/d)}\equiv 4^{\phi(n)}\begin{cases}(\mathrm{mod}\ n^3), & \text{若 } 3\nmid n\\ (\mathrm{mod}\ n^3/3), & \text{若 } 3\mid n\end{cases}$$

其中 $\phi(n)$、$\mu(n)$ 分别为欧拉函数和莫比乌斯函数。当 n 为素数时，此即著名的莫利（Morley）定理。

二次型是高斯著作中的重头戏，尤其是表整数问题，拉格朗日证明了，每一个自然数均可表为 4 个整数的平方和。本书这方面谈的不多，但对于著名的华林问题，我们却有独到深刻的描述。设 k 和 s 为正整数，考虑丢番图方程

$$n=x_1+x_2+\cdots+x_s\ .$$

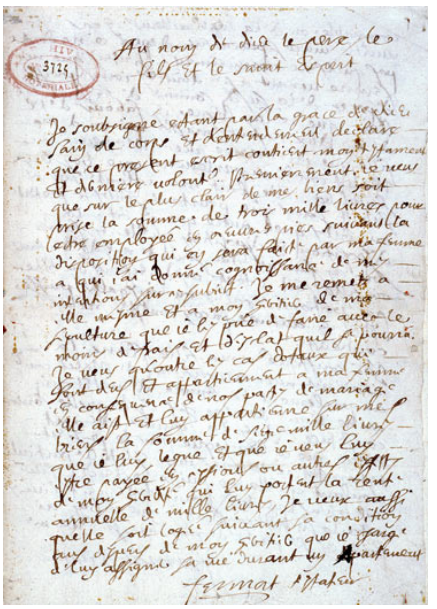
其中

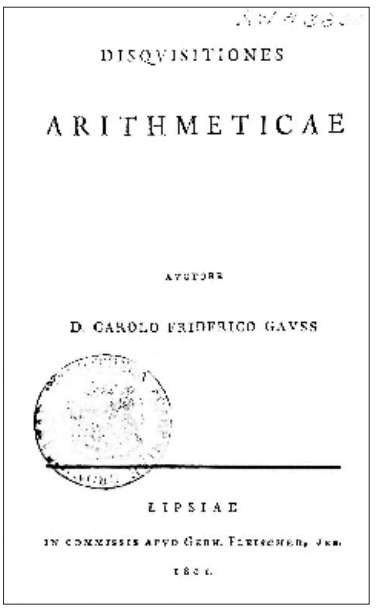
$$x_1x_2\cdots x_s=x^k$$

由希尔伯特 1909 年的论证可知，必定存在 $s=s'(k)$，使对任意的正整数 n，均可表成不超过 s 个正整数之和，且其乘积是 k 次方。用 $g'(k)(G'(k))$ 分别表示最小的正整数 s，使对任意（充分大的）正整数 n，上述方程成立。我们在第 7 章给出了 $g'(k)$ 的准确值和 $G'(k)$ 的估值，同时猜测 $G'(3)=3$, $G'(4)=4$。一个更为精巧的推测是，除了 2、5 和 11，每个素数均可表成 3 个正整数之和，它们的乘积为立方数。

之所以能提出这类问题，是因为我们把整数的加法和乘法结合起来考虑，这一点受到了 abc 猜想的形式启发，后者可以轻松导出费尔马大定理等一系列著名


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, viâ Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS




DISQVISITIONES
ARITHMETICAE
AVCTORE
D. CAROLO FRIDERICO GAVSS
LIPSIAE
IN COMMISSIS APVD GERH. FLEISCHER, JUN.
1801.

古典大师书影手迹三部：丢番图《算术》拉丁文版首版；费尔马亲书遗嘱，要求销毁手稿；高斯《算术研究》初版

猜想和定理，其在数论领域的影响力迅速替代了已被证明的费尔马大定理。事实上，毕达哥拉斯的完美数和友好数问题也是这两种基本运算的结合，它们具有恒久的魅力。正是从这里开始，我们的想象力获得提升，渐渐脱离开了同余的观念。

除了新华林问题，我们把著名的费尔马大定理也做了推广（第 7 章第 3 节），即考虑丢番图方程

$$\begin{cases} a+b=c \\ abc=x^n \end{cases}$$

的正整数解。设 $d=gcd(a,b,c)$，当 $d=1$ 时，该方程等同于费尔马大定理。也就是说，无正整数解。而当 $d>1$ 时，方程的可解性存在各种可能性，比如 $d=2$, $n=4$ 时有解 $(a,b,c;x)=(2,2,4;2)$。这就提出了一个新问题，我们的猜测之一是，当 d 和 n 均为奇素数时，上述方程无解。这是费尔马大定理的完全推广，且无法由 abc 猜想导出（已有的两个推广——费尔马 - 卡塔兰猜想和比尔猜想则可由 abc 猜想轻松推出）。

高斯在 19 岁那年证明了：每个自然数均可表示为三个三角形数之和。这是对费尔马问题的第一个回答，后者在丢番图的《算术》空白处写下了第 18 条注释：当 $n\geq 3$ 时，所有自然数均可表示成 n 个 n 角形数之和。所谓 n 角形数是毕达哥拉斯学派定义的，即正 n 角形中的角点个数。特别地，三角形数为 0, 1, 3, 6, 10……即所有形如 $\binom{x}{2}$ 的二项式系数，其中 10 和 21 分别为保龄球的木瓶和斯诺克的目标球的排列方式和数目。

我们注意到了，二项式系数有着特殊而奇妙的性质，它是除了数幂以外最简洁的整数，因此值得数论学家重视。二项式系数以及多项式系数在本书中多次出现，我们甚至定义了形素数 $\binom{p^i}{j}(i,j\geq 1)$，这是一类特殊的二项式系数，将素数与形数结合起来，其个数与素数个数在无穷意义上是等阶的。我们猜测（已验证至 10^7）

任意大于 1 的自然数均可表示成 2 个形素数之和。

这个猜想的提出无疑受到了哥德巴赫猜想的启发。后者说的是，每个大于等于 9（6）的奇数（偶数）均可表示成 3（2）个奇素数之和。我们认为，这一点不够一致，且素数本身是构成整数乘法意义的基本单位，用在加法上未必是最佳选择。另外，随着数的增大，它的表法数也越来越多，似乎颇有些浪费了。与此同时，我们也提出了下列弱孪生素数猜想：

对于任意正整数 k，存在无穷多对相邻为 $2k$ 的形素数。

我们研究的最古老的数学问题是完美数问题，这是古希腊数学家毕达哥拉斯开创的问题。毕达哥拉斯考虑了自然数的真因子之和等于其自身的那些数，即满足

$$\sum_{d|n,d<n} d=n,$$

他称其为完美数。例如 6 = 1+2+3，28 = 1+2+4+7+14，经过阿契塔和欧拉（相隔 1200 年）的努力，得知偶数 n

高斯故乡不伦瑞克街景（蔡天新 摄）

数学王子高斯诞生地（蔡天新 摄 ）

是完美数的充分条件是 $n = 2^{p-1}(2^p - 1)$，其中 p 和 $2^p - 1$ 均为素数。这样的 p 也叫梅森素数，利用最现代的计算机可以得到 48 个梅森素数，也就是说，我们已知 48 个完美数。另一方面，包括笛卡尔、费尔马和欧拉在内的数学家曾考虑过诸如 $\sum_{d|n,d<n} d = kn$ 之类的推广，但都只获得若干特解。我们考虑了平方和的情形，即

$$\sum_{d|n,d<n} d^2 = 3n,$$

得到了上式成立的充要条件是 $n = F_{2k-1}F_{2k+1}$，其中 F_{2k-1} 和 F_{2k+1} 是斐波那契孪生素数，从而再次产生了无穷性。由目前的计算机只能求得 5 对，即有 5 个平方和的完美数，后面 2 个已经是天文数字。有趣的是，这 5 个完美数既有偶数也有奇数。但对于非 3 常数或立方及更高幂次的情形，这一现象不再出现。

本书的前五章和第 7 章补充读物构成了《初等数论》课程的教学内容，可供大学数学系每周四次的教学之用，最后两章不在《初等数论》教程的讲授范围之内，但它们与同余式紧密相关，且能够伸手触摸到，也可算是本教材的一大亮点。至于本书的最大特色，可能要数每节正常内容后面的补充读物（可以选讲，未安排习题）。这种形式是一种尝试，希望借此拓广读者的知识面和想象力，递增他们对数论的兴趣和热爱。事实上，这些补充读物至少有两个功能：

其一，介绍了其他数论问题和研究的初步知识，例如欧拉数和欧拉素数，阿达玛矩阵和埃及分数，佩尔方程和丢番图数组，阿廷猜想和特殊指数和，椭圆曲线和同余数问题，自守形式和模形式，等等。其二，介绍了与初等数论相关的新问题和新猜想，除前面提到的以外，还有格雷厄姆猜想，$3x+1$ 问题，广义欧拉函数问题，覆盖同余式组，素数链和合数链问题，卡塔兰猜想，多项式系数非幂，等等。

可是，也正因为问题和猜想比较多（有时较为大胆），容纳了本人的研究经验，尤其是近年来的思考（有的尚未发表），错误在所难免（并非客套），期望读者予以发现和纠正。本书的写作也是对过去 25 年来教授浙江大学《初等数论》课程的小结，部分内容包括习题的选取得到了近十位研究生和合作者的帮助，恕不在此一一提及名字，他们参与研究的某些工作和国内外许多同行的相关成果在书中有所展示。值得一提的是，不少工作的进展和预测得到了计算机的帮助，这是我们比前辈同行优越的地方。可以说，计算机之于数论学家，犹如望远镜之于天文学家。

除此以外，我要特别感谢前辈数学家王元先生，他不仅为本书题写了书名，同时在许多方面予以支持和鼓励。还有菲尔兹奖得主、剑桥大学教授阿兰·贝克和卡塔兰猜想的证明者、哥廷根大学教授普莱达·米哈伊内斯库的褒奖，前者称赞新华林问题是“真正原创性的贡献”，后者勉励作者“在当今繁杂的数学世界找到了一片属于自己的领地”。

最后，我想引用高斯的一段话作为结束语，摘自他为英年早逝的弟子艾森斯坦的论文集所写的导言：“数论提供给我们一座用之不竭的宝库，储满了有趣的真理，这些真理不是孤立的，而是最紧密地相互联系着。伴随着这门科学的每一次成功发展，我们不断发现全新的，有时是完全意想不到的起点。算术理论的特殊魅力大多来源于我们由归纳法轻易获得的重要命题。这些命题拥有简洁的表达式，其证明却深埋于斯，在无数徒劳的努力之后才得以发掘；即便通过冗长的、人为的手段取得成功以后，更为清新自然的证明依然藏而不露。”

2012 年夏天初稿
2013 年元旦修改